Spring 4-1-2008

Reference Guide for K12 Network and Information Administrators

Anders Berggren
Dakota State University

REFERENCE GUIDE FOR K12 NETWORK AND INFORMATION ADMINISTRATORS

A graduate project submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Master of Science

in

Information Systems

April 2008

By
Anders Berggren

Project Committee:

Dr. M. Moran
Dr. X. Fu
Dr. S. Krebsbach

PROJECT APPROVAL FORM

We certify that we have read this project and that, in our opinion, it is satisfactory in scope and quality as a project for the degree of Master of Science in Information Systems.

Student Name: Anders Berggren

Master's Project Title: Reference Guide for K12 Network and Information Administrators

Faculty supervisor:_____ Date: _____

Committee member:_____ Date: _____

Committee member:_____ Date: _____

ACKNOWLEDGMENTS

The completion of this project would not have happened without the encouragement and support of many individuals.

- Dr. Sharon Neet, Lynnette Mullins, Dr. Bernard Selzler, Dr. Christo Robberts, and Dr. David DeMuth for their persistence, guidance, support, and editing.
- The Northwest Service Cooperative and the K12 school districts in northwestern Minnesota for sharing information with me.
- My mom for sharing her love of education with me.
- Curtiss Wikstrom and Wikstrom Telephone Company for the many I/T leadership opportunities.

ABSTRACT

Through personal observation, it was determined that K12 school districts in northwestern Minnesota were using a non-scientific, ad-hoc approach to managing their I/T resources. These observations were confirmed through literature produced by the Minnesota Department of Education and through surveys conducted with K12 school districts in northwestern Minnesota. This ad-hoc style of I/T management created areas where districts were not operating within federal and state regulations and were not meeting K12 and I/T federal or state objectives.

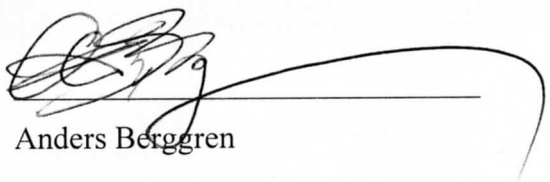
It was determined that staff managing I/T resources in K12 school districts in northwestern Minnesota have training in education and technology, but not management. As a remedy, a training plan and training materials were developed. This training is necessary in order to promote a policy-based management style. While many policies to enforce regulations are discussed, there is emphasis placed on the technology plan. Technology plans are a policy which K12 districts are already required to have in order to receive various federal and state funding.

DECLARATION

I hereby certify that this project constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the project describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,



Anders Berggren

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Background of the Problem

While consulting with six school districts (Crookston Public Schools, Fisher Public Schools, Kittson Central Public Schools, Tri-County Public Schools, Warroad Public Schools, and Crookston Cathedral School), and personal communications with nine additional school districts (Thief River Falls Public Schools, Marshall County Central Public Schools, Greenbush-Middle River Public Schools, Stephen-Argyle Public Schools, Warren-Alvarado-Oslo Public Schools, Badger Public School, Roseau Public School, Kelliher Public School, and Fosston Public School) in northwestern Minnesota, it was clear that there was not a formal management style being used with respect to Information Technology (I/T). In these districts there is an ad hoc approach to managing I/T where responsibility, budgeting, staffing, and accountability are dealt with on a case-by-case basis. This ad hoc approach has created a degree of separation between practice and what federal and state laws are mandating.

There are several common characteristics between these districts. Some of the more significant characteristics are:

Regional Location: All fifteen of the schools encountered, are in close proximity to each other (see Figure 1). As of the 2007-2008 school year, there are thirty-nine school districts in the eleven counties in northwestern Minnesota.

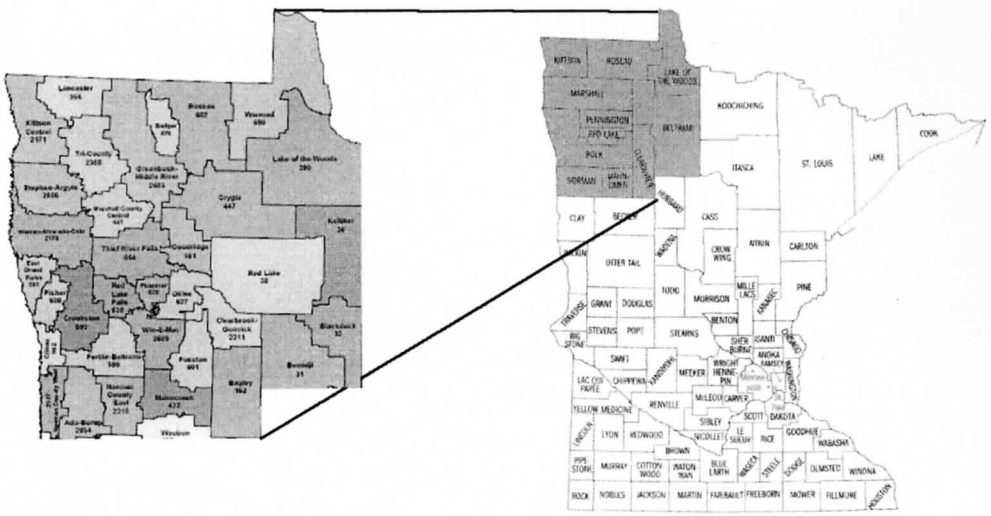


Figure 1: Northwestern Minnesota Counties and School Districts (Minnesota Department of Education [MDE] 2008a; U.S. Census Bureau [USCB] 2008a)

Declining Population: Of the eleven counties in northwestern Minnesota, there has been an average decline in population of 2.8 percent from the 1990 Census until the 2006 Census estimates (see Appendix B). Counties such as Kittson and Marshall, without major employers, have suffered greater losses as people have moved to communities in Beltrami, Roseau, Pennington, and Polk counties where employment opportunities are greater. (Minnesota Department of Employment and Economic Development [MDEED] 2005a; MDEED 2005b)

Economic Status: The major industries in this region are manufacturing and retail. The average wage is roughly $12.60 an hour. Regarding I/T positions in this region, the Minnesota Department of Employment and Economic

Development (2005a; 2005b) report an average wage of $20.62 an hour for "Computer and Mathematics" positions and $30.35 an hour for "Management" positions.

Open Enrollment: Minnesota has an open enrollment policy where families do not have to attend schools based upon where they live, but may choose which school to attend; however, there are district boundaries, and the school district does still have responsibility for those families. This does create some opportunities for competition between districts. An example of this is the Fisher Public School; parents are attracted to it because of the small class sizes. Fisher School has so many students attending from within the Crookston district that it has two bus routes to pick up students in Crookston.

There are drawbacks to open enrollment; it has created administrative overhead and financial burdens on some districts. When a student attends a neighboring district, the neighboring district gets the state paid tuition for that student. When a special needs student attends a neighboring district, the neighboring district gets the state paid tuition and an additional assessment is charged to the home district to defray any expenses that may occur (for additional support staff, equipment, or other financial burdens the neighboring district may incur for that student).

Participation in an Educational Service Cooperative: All of the districts are able to receive similar services from the Northwest Service Cooperative

(NWSC), which provides cooperative purchasing, training, and monthly professional development meetings for technology staff and administration. The monthly meetings are held at the NWSC office in Thief River Falls, Minnesota and via IP-videoconference. These meetings serve both training and information sharing. The majority of the training is of a technical nature or is provided by sales engineers as a way to market products. There is also a listserv managed by the service cooperative for information sharing.

The NWSC also hosts a yearly technology conference at the University of Minnesota, Crookston campus. This conference is attended by technology coordinators, principals, superintendents, and representatives of local government. There are two focuses of the conference, demonstrating new I/T products and services and hands-on training for the use and management of I/T products and services.

Declining Enrollment: Most areas of northwestern Minnesota have experienced population loss, but all of the schools in northwestern Minnesota have experienced significant (between 6% and 40%) decreases in enrollment (see Appendix B). There has not been a statewide redistricting in more than 30 years, but as schools continue to drop in enrollment, consolidations occur more frequently.

Independent School Districts: Minnesota school districts are independently operated. The Minnesota Department of Education (MDE) provides

> motivation for technology planning. As independent districts, there is no central purchasing or decision making with respect to technology. Each district is maintaining business office software, student information systems, content filtering, and all other technology systems. MDE does require regular reporting of financial and high-level student progress data, and there are a limited number of approved student information system and financial management software vendors capable of producing these reports, so K12 districts do have a limited number of choices.

Minnesota K12 schools have a history of being innovators and leaders in I/T deployment and curriculum integration. During the 1970's, the Minnesota Educational Computing Consortium (MECC) was formed. Answering demands from the Minnesota Governor's office, MECC provided I/T budget and management oversight. At the same time MECC provided access to time-share computing systems (providing both hardware and telecommunications resources), developed educational software, and coordinated cooperative purchasing bids for microcomputers. As time-shared systems were replaced by microcomputer systems in the 1980's, school districts demanded local control of I/T. MECC relinquished control of budgets and management to local districts and became a software publishing company. Individual teachers and principals in many smaller districts championed I/T projects and were given roles of managing I/T resources as a result (O'Neill 1995).

Many Minnesota K12 school districts have hired full-time technology staff (one or more individuals dedicated to I/T departments), while others are relying on a teacher or principal to manage the district's I/T resources in addition to their regular duties. Even in the

districts with a full-time technology staff, educational backgrounds vary from I/T technician, to teacher, or to someone self-trained with little formal education. This is evident in the districts in northwestern Minnesota, as there are one-man technology departments and teachers who are part-time I/T staff in the majority of the districts. The independent districts have made unique decisions regarding I/T, and there are enormous gaps between districts in areas such as telecommunications infrastructure, access to computers, access to Internet-enabled computers, technology-integrated curriculum, and available software. Districts have developed their own ad hoc approach to managing technology, which has helped them get by, but does not maximize potential.

As a result of the ad hoc styles of management, each district has its own issues. One district had previously operated with a deficit and now business office personnel prefer to overcompensate by spending as little as possible from the allocated technology budget. One has defined that students are not allowed to use email or social networking sites as part of their acceptable use policy, but uses a case-by-case decision for enforcing punishment. This varies from ignoring the offense to in-school suspension. Several of them have weak password policies, and also use web-accessible student information systems without SSL or similar encryption, which is negligent and does not comply with federal and state regulations. This does open the district up to liability issues for not properly securing private data.

Statement of the problem

All of the K12 districts in northwestern Minnesota are still using an ad-hoc approach to managing I/T including spending, staffing, and training. This has inadvertently created

areas of non-compliance. There is a lack of training opportunities for K12 school district I/T staff in areas of using policy to automate management (policy-based management).

There are areas where the ad hoc management style employed by K12 districts has created non-compliance with federal and state regulations. These are:

1. Lack of defined and enforced security plans. This includes password complexity policies for accessing private data; not requiring a level of encryption for the storage or remote access of private data; and lack of training plans for district staff regarding the use of private data.
2. Lack of defined and enforced privacy, data retention, and incident response plans. This includes knowing what data is being stored and how long the data needs to be stored; notifying persons whose data is stored if it is accessed inappropriately; and proper destruction of data when it is no longer needed.

By not developing and enforcing a realistic technology plan, K12 schools are not meeting or exceeding federal and state objectives. The technology plan is to be used for budget, asset management, technology implementation, and reporting where a district is currently using I/T. The technology plan is currently a burden for most districts, as it is only created to qualify for federal telecommunications funding. It must be revised every three to five years, and is not generally referred to or revised outside of required revision periods.

Objectives of the project

The areas where K12 districts are not in compliance with federal and state regulations or are not exceeding federal and state objectives are easily resolved. Policy-based

management training is not available or existing training is considered non-relevant. Policy-based management training material was created for K12 district I/T staff as part of this project. This was done through the creation of a handbook which would provide some direction when creating policies and using them.

After collecting and reviewing data from a survey, conducted in April of 2006, it was realized that the lack of knowledge, in regulations impacting K12 I/T and policy-based management, was much larger than originally anticipated. A handbook was created as originally planned and a larger-scope training plan was also developed. The training plan includes an initial implementation schedule. The handbook will be an integral part of the first phase of training.

LITERATURE REVIEW

Minnesota Department of Education (MDE) technology plans and federal and state regulations related to I/T and K12 were reviewed. The federal and state regulations set standards in areas such as privacy, security, accountability, and objectives. Some of the regulations require documentation of compliance, generally by policy. For example in order to receive telecommunications assistance under the Communications Act, form 479 must be submitted. This form is used as verification that the Children's Internet Protection Act (CIPA) is being followed. CIPA requires that an Internet Safety Policy exists. Other regulations do not require documentation, but having a policy, which addresses the regulation, in place and enforced is a successful method for guaranteeing compliance.

Existing and recent legislation such as the Family Educational Rights and Privacy Act of 1974 (FERPA), No Child Left Behind Act of 2002 (NCLB), and even those not directly related to education such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) Sarbanes-Oxley Act of 2002 (SOX) or Gramm-Leach-Bliley Act of 1999 (GLBA) are initiating changes in the way educational institutions manage information and technology. (US Department of Education [USDE], 2005a; USDE, 2005b; US Department of Heath, 1996) There are definitions set on privacy rights for students and families, correctness of financial information, and accountability for student success.

Universities and colleges are following the new guidelines imposed by GLBA, due to the financial transactions that they are involved with. The University of Minnesota, for

example, has initiated a training program called "Public Jobs: Private Data" for its employees. The goal of the program is to help employees determine what is and is not non-public information and how to handle it, in order to comply with GLBA, HIPPA, FERPA, and the Minnesota Data Practices Act. (University of Minnesota Controllers Office, 2003)

SOX focuses on the correctness of a publicly traded company's finances with respect to its shareholders. SOX sets a level of accountability for management. Management becomes dependent on I/T departments to ensure that only those who need to access data can do so, and only those who need to modify data can do so. Ultimately I/T departments must ensure that accounts with proper permissions can only be used by the individuals assigned to them through the use of strong passwords or other authentication mechanisms. (AICPA, 2005) While this does not directly impact education, as public institutions, K12 school districts should hold themselves to the same level of accountability. As a taxpayer funded organization, the correctness of financial data is just as critical as a publicly traded company. Additionally, the correctness of information regarding student achievement is important. The student will use this data in the future for further education and employment.

Information technology professionals everywhere are being required to provide assurance to management that systems are secure and that policies are in place to minimize damage done to the organization in the case a security event should occur. With respect to information technology security and education, EDUCAUSE (2005) has published a list of best practices for security in higher education environments. These include education, training, and awareness campaigns; performing risk assessments; and developing security strategies that include both technological and non-technological (training) approaches.

Another front that educational institutions must protect is academic integrity. As online learning proliferates, it becomes increasingly difficult to minimize the risks of academic dishonesty. Baron and Crooks (2005) identify issues with enforcing academic integrity and online learning as well as several best practices to minimize dishonesty. Some approaches are increased interaction between student and faculty (as a method of recognizing writing style), using proctors for exams, using plagiarism detection tools, or altering assignments on a rotation.

Garthwait and Weller (2005) discuss how technology is being utilized in K12 classrooms in Maine. Maine started a one-to-one laptop to student initiative in 2002. There are best practices and obstacles documented from two teachers who have been forced to integrate technology into their curriculum.

The state of Minnesota has set goals for K12 I/T spending during the 2008—2009 budget year. These were based on Governor Pawlenty's world-class students initiative, "From nation leading to world competing", which includes one-time I/T upgrades. These upgrades are to standardize technology across Minnesota schools, including purchase of hardware or software. It has been identified that there are gaps between districts in the age of I/T equipment and the availability of quality telecommunication service providers. This funding is an attempt at standardization (Minnesota Department of Education [MDE], 2008b).

MDE has also set expectations for K12 districts in a state technology plan. This plan integrates components of the National Technology Plan and the Minnesota Digital Learning

Plan (an initiative which included higher education and public libraries), but focuses on issues specific to K12 schools in Minnesota. There are state-wide deficiencies defined such as lack of uniform access to I/T resources across the state; lack of training required for faculty in technology integration; difficulty of reaching a minimum level of conformity in areas such as available resources and training due to independent nature of Minnesota K12 districts; range of I/T expertise between districts; districts using obsolete I/T equipment as part of a piecemeal approach to asset management; lack of information sharing between districts and MDE due to software incompatibility; and lack of well designed security plans for private data. There are also goals such as defining training opportunities in a statewide clearinghouse system; requiring minimum technology training requirements for both faculty and administration; increasing the amount of information sharing between districts and MDE through the use of standardized data formats; and standardization of access to I/T resources across the state. The state technology plan also notes the importance of the district technology plans and the lack of effort some districts put into the creation and enforcement of them (MDE, 2005).

Minnesota schools state-wide are facing similar issues to those observed in northwestern Minnesota. Minnesota schools are not alone when facing federal accountability regulations such as NCLB or identifying areas for curriculum integration. As state funding for I/T is being changed, it is critical that districts make plans to effectively budget so district, state, and federal goals are achieved.

SURVEY METHODOLOGY

A survey was used to analyze respondents' knowledge of regulations and the use of policies in K12 districts. The survey was conducted using the WebTools system at the University of Minnesota, Crookston campus (UMC). The survey software was developed by Dr. David DeMuth and has been used for educational research projects including Dr. Steven Shirley's dissertation, *The gender gap in post-secondary study abroad*, and a study of the Crookston community regarding their perceptions of a Wal-Mart opening in Crookston..

The survey consisted of six Likert item questions: two were to determine respondent background information, position and years in current position; three were related to the knowledge of laws and use of policies in their district; and a final question was used to determine if there was interest in receiving training regarding policies and policy-based management styles. Background information included the type of position and number of years employed in that position. Knowledge of laws and use of policies included understanding of several laws, identifying whether or not a policy exists and is enforced, and an opinion of whether or not their district effectively employ I/T policies. The survey tool can be found in Appendix B.

The survey was conducted during April of 2006 and was made available to 15 of the K12 school districts in northwestern Minnesota. The 15 school districts were the six districts that were consulting clients and the nine districts that had previous personal communication. Original intentions were to use the districts already receiving consulting services and those

who already had open communication as the initial targets for the training produced by this project. These districts vary in size and are primarily along the very northwestern corner of Minnesota. The survey was emailed to technology coordinators in each district.

There were 8 of the 15 districts who responded to the survey (a 53% response rate). In the 11 counties of northwestern Minnesota, there are a total of 39 school districts. Therefore, there was a 20% sample of the total number of districts. While a 20% sample is not large, the results align with personal observations and information gathered from literature.

SURVEY RESULTS

Demographic Information

The majority of the respondents identify themselves as technology staff. There were five respondents who identify themselves as technology staff, two respondents who identify themselves as faculty, and only one who identified himself as being part-time administration. At the same time the majority of respondents have been employed in their current position for more than six years. Table 1 correlates the responses between role and duration.

Table 1: Relationship between role within K12 school district and number of years employed.

		Role Within District		
		Technology Staff	Faculty	Other
Years in current position	< 1	1	-	-
	2 - 4	-	-	-
	4 - 6	2	-	-
	> 6	2	2	1*

*Other response was: "Technology Coordinator about 80% tech and 20 admin"

Knowledge of Regulations

Five federal regulations which contain statements impacting I/T in K12 school districts were presented: Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy and Protection Act (COPPA), Children's Internet Protection Act (CIPA), Gramm-Leach Bliley Act (GLBA), and Sarbanes-Oxley Act (SOX). The respondents were asked to identify how well they understood each regulation and how it could be applied to K12 school district I/T. For this question a four-point Likert scale would have been more

indicative, as there was a strong Neutral bias. Figure 2 summarizes the responses to the knowledge questions.

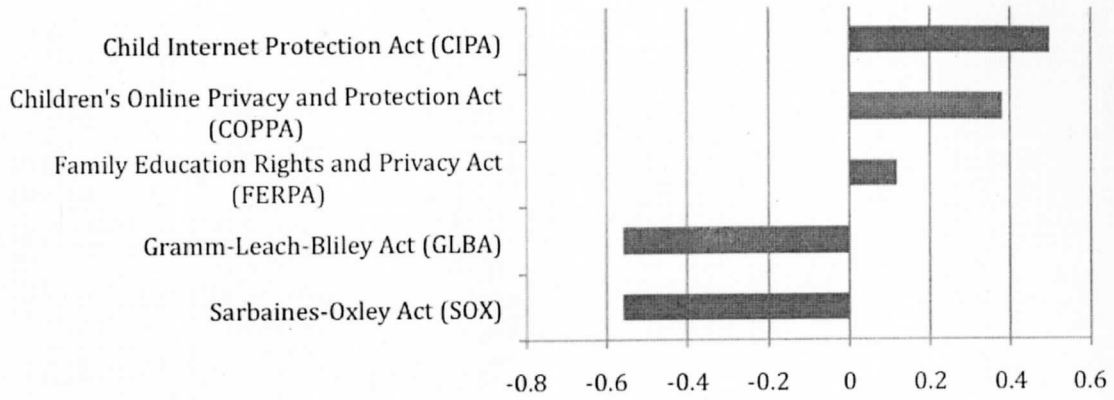


Figure 2: Understanding of Regulations and Their Impact on K12 I/T

CIPA had the strongest agreement that the respondent was familiar with the regulation and how it could be applied to the district. This was expected, as CIPA compliance is required in order for K12 school districts to receive federal telecommunications funding. It was alarming to see that more of the respondents agreed that they understood COPPA and its impact than FERPA, which has existed 24 years longer than COPPA and directly deals with educational institutions. Table 2 details the relationship between respondents who claim to have weak understanding of FERPA and how long they have been in their current position.

More alarming than the fact that there was not a strong understanding of FERPA was the respondents who did not understand FERPA and how it could relate to I/T had been employed in their current positions longest. This is evidence that there has not been continuous discussion and training for staff in the handling of private data.

Table 2: Relationship between FERPA knowledge and number of years employed.

		Understanding of FERPA and how it could be applied to district and technology				
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Years in current position	< 1	1	-	-	-	-
	2 - 4	-	-	-	-	-
	4 - 6	-	-	1	1	-
	> 6	-	2	2	1	-

There was less knowledge of both GLBA and SOX and how it could be applied to I/T in K12 districts, which is understandable as they are fairly recent regulations. Neither of them directly deals with education but have to deal with accountability of administration and the correctness of data.

Use of Policies

The first question was to determine the use of policies to provide direction to I/T staff. There was a large neutral bias with this question, but none of the respondents agreed that there were policies which provided direction to I/T staff (see Figure 3). The second question was to determine if specific policies existed and if they were followed. This could have been broken into two questions, but was not because it was assumed that if a policy was not enforced it might as well not exist.

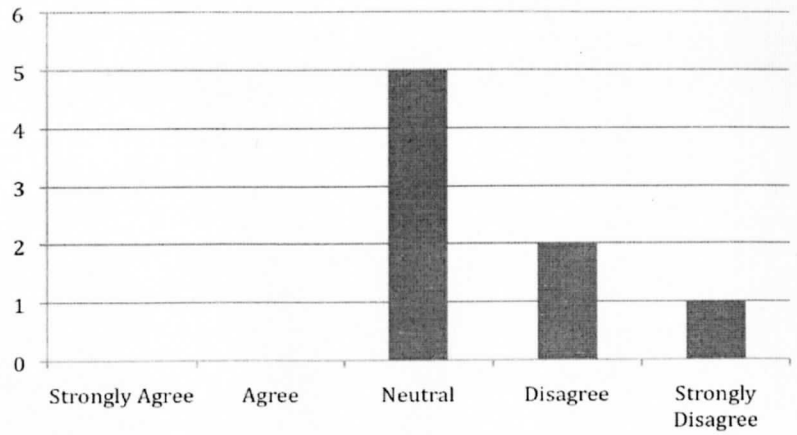


Figure 3: Usage of Policies Providing Direction to I/T Staff

The policies presented can be broken into two categories: policies which dictate the behavior of end-user and policies which dictate the behavior of I/T staff. End-user policies included acceptable use, Internet safety, privacy, and password. I/T staff policies included data retention and destruction, disaster recovery, incident response, security, and technology plan. There is stronger agreement to the existence and usage of end-user policies compared to I/T staff policies. This enforces the results of the previous question. Figure 4 summarizes the responses for each policy.

In order to qualify for federal telecommunications funding, districts are required to have a current technology plan on file and comply with the CIPA, which requires an Internet safety policy. As districts are required to have a technology plan, it can be assumed that the responses regarding the technology plan only indicate whether or not it is enforced in their district. All of the respondents agree with some level of certainty that their district does have an acceptable use and/or Internet safety policy.

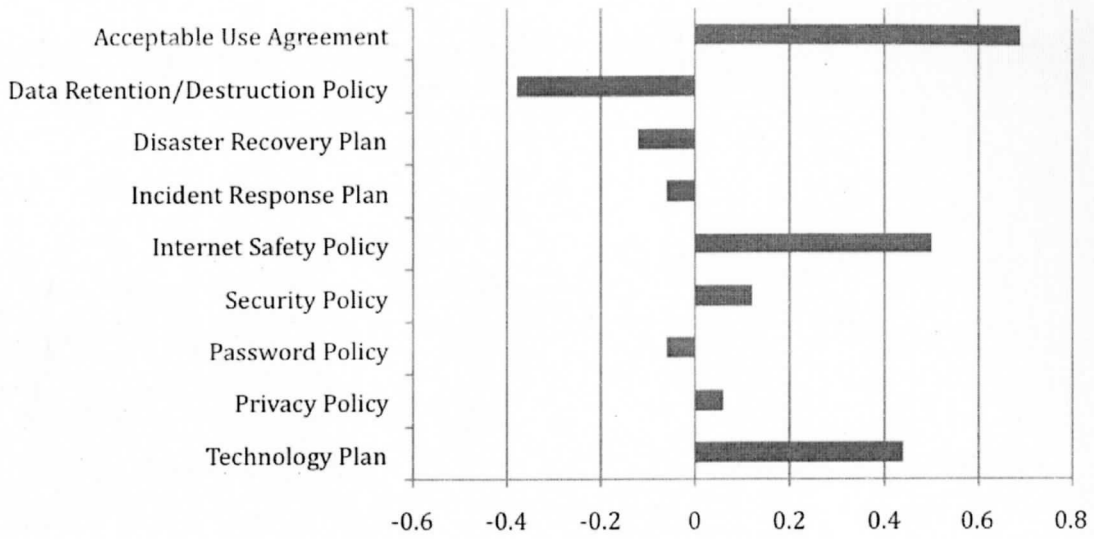


Figure 4: Existence and Enforcement of Specific Policies

There were two respondents who disagree with the statement that their technology plan is enforced. One respondent was technology staff and the other was faculty.

Interest in Policy-Based Management Training

There is evidence that the respondents are interested in training. The majority of respondents, seven out of eight, indicated with a strong level of agreement that they were interested in receiving training related to I/T policies. The interest in training ranged from those who were new to their positions, through those who had been in their position for more than six years.

Table 3: Relationship between interest in training and number of years employed.

		Would you be interested in receiving training related to I/T policies?					
		Abstain	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Years in current position	< 1	-	1	-	-	-	-
	2 - 4	-	-	-	-	-	-
	4 - 6	-	1	1	-	-	-
	> 6	1	3	1	-	-	-

Summary

There were several trends which support the need for additional training that were discovered while analyzing responses. These were:

- Policies required to receive federal telecommunications funding exist, but are not necessarily enforced.
- There was a less than adequate level of understanding of regulations such as SOX and GLBA. Both SOX and GLBA mandate the existence of privacy policy, password policy, disaster recovery plan, and incident response plan. These policies were non-existent or not enforced in the majority of districts.
- Policies which provide direction for specific issues such as a password policy, data retention and destruction policy, and incident response plans do not exist or are not enforced.
- Policies which provide direction for district-wide initiatives, such as the technology plan exist, but are not executed or are ineffective.
- Regardless of role within the district or the number of years employed, there is a need for training or information sharing regarding regulations and policies which should exist for compliance with those regulations.

- Regardless of role within the district or the number of years employed, there is interest in additional training opportunities in the area of policies and K12 I/T.
- The target audience for training is technology staff, who may also be faculty or part-time administration.

CONCLUSION AND DISCUSSION

Minnesota K12 school districts have a legacy of pioneering computer use in the classroom and availability to the district. K12 school districts in northwestern Minnesota are being faced with many issues such as population and enrollment declines, consolidation, and students enrolling in competing districts. With legislation such as No Child Left Behind and Governor Pawlenty's "Nation Leading to World Competing" campaign, funding will only be available to districts who are able to perform with unparalleled effectiveness. In order for K12 districts in northwestern Minnesota to receive funding for future I/T initiatives, they will need to demonstrate that they are effective programs which will be unique to the state and nation.

Based on information observed, literature from the MDE, and data collected from surveys, K12 school districts in northwestern Minnesota are in need of training in order for them to have effective I/T management. Survey data indicated there was strong interest from at least 7 of the 39 districts in northwestern Minnesota (18 percent). This number is likely understated due to the small sample size of the survey, but indicates that developing relevant training material would be useful.

The proposal is to produce training material in four phases:

I. Policy-Based Management

Encourage development of management skills. Most of the technology leaders in the target schools are not administrators, but instead have a computer science or teaching background.

II. Staff Development

Locate valuable technology proficiency and curriculum integration training for district staff. This training could be developed in-house, purchased from professional trainers, or purchased from regional higher education institutions.

III. Technology Integration

Develop realistic and progressive technology integration and immersion plans, which align themselves with district technology plans.

IV. Accountability

Develop metrics and measure performance. Assist with creating measurement tools, which are unique and measure the goals of each district. Areas of focus would include spending, training, and community service.

Phase I

Phase I will begin with developing training sessions aimed at incorporating a policy-based management style into K12 school district I/T staff in northwestern Minnesota. The training will include several sessions with technology staff to develop effective policies. Training will start with policies having a smaller scope such as password complexity, acceptable use, data retention, and privacy. Gradually we will work toward policies with larger scope which focus on objectives, such as the district technology plan. The primary

audience for phase I will be technology staff and administration. The emphasis will be on technology staff, but in order for districts to successfully employ a policy-based management style in their I/T departments, there will need to be buy-in from administration.

A handbook (Appendix D) was developed to aid with this training. The purpose of this handbook is to detail existing regulations, how they may be applied to K12 school districts, a primer on developing policies using a policy development lifecycle, and example policies. It also discusses some of the policies that should exist to address areas of the regulations. This is not the only resource which will be distributed as part of training. The following resources developed by other organizations will be distributed as part of training:

- Minnesota Department of Education Technology Planning Guide for Minnesota School Districts—This is an online document which is updated every three years. It sets forth minimum specifications for district technology plans. The MDE holds informational sessions with school districts regarding the technology plan, these sessions are only held every three years and have not encouraged districts to use the technology plan to the maximum potential.
- Minnesota Department of Education State Plan for Technology in K12 Education—This statewide plan sets the goals of the state of Minnesota in regards to technology in K12 education. This is an excellent resource because aligning district goals with state goals, especially in the case of new or unusual initiatives, can lead to additional funding opportunities. This is also an online document which is updated every three years. This does not use the same three year cycle as the Technology Planning Guide.

- SAGE Guide to Developing Computer Policy Documents—This booklet goes into detail on the topic of developing I/T policies. As a SAGE member, these booklets can be purchased for $10.00.

The intentions of this project are to introduce policy-based management training to technology staff early in the fall of 2008. The Northwest Service Cooperative has yearly technology conferences in April. Both technology staff and administration attend this conference, and the 2009 conference will be an opportunity to approach staff and administration regarding policy-based management and staff development.

Phase II

The second phase will be to focus on development of teaching staff in areas such as technology literacy, technology integration, and innovation. This phase should be completed at roughly the same time as Phase I. Having a highly developed teaching staff will promote technology use. If resources, such as computer labs, are being used at their maximum capacity, it can be easier to justify expanding those resources. Having a "if I build it, they will come" attitude toward spending in K12 school districts is not effective. Before a district can and should budget for the amount of resources required to support K12 technology integration, there needs to be evidence that it is possible. Some staff will have to be trained and start using technology. There are some districts who have staff capable of developing training for technology integration. They can be an excellent resource for the district, but some other opportunities for training include:

Computer Use

- Northland Technical and Community College (East Grand Forks, MN and Thief River Falls, MN)—Offerings include: word processing, spreadsheets, databases, graphics and desktop publishing, webpage development, operating systems, and PC troubleshooting training.
- University of Minnesota, Crookston (Crookston, MN)—Offerings include: Microsoft Office training and MOUS certification.
- Northwest Service Cooperative (Thief River Falls, MN)—Offerings include: Microsoft Office, iPod and podcasting, iMovie, Garage Band, and SMARTboard training.

Technology Integration

- SchoolKiT—Provides services such as edClass, classroom-ready technology integration activities and pdPoint, online professional development of teachers in areas such as technology integration.
- Apple Learning Interchange—A social network for teachers who have developed technology integrated curriculum.

External training opportunities are abundantly available and are of excellent quality. Obtaining the qualifications and personally developing these training resources would not be feasible. Getting technology staff to connect faculty with training resources is feasible and necessary before moving on with Phase III, developing technology integration plans. Faculty should be developed at the same time technology staff is being developed. The proposed method for training faculty is:

1. Get a team of faculty. Having a team who are already technology champions may be the easiest, but not necessarily most successful. Areas of focus from the Governor's plans would be math and science.
2. Focus on training this team. First focus on standardizing the groups' level of technology literacy. Then focus on integrating technology into their classrooms.
3. Have these teachers share best practices and results with others as a means of motivation.
4. Expand training to a larger team of faculty, integrating with mentoring already done in many districts.
5. Continue to provide training opportunities for those who already have been trained. Without constant improvement and motivation, there is a chance that those who have been trained will become stagnant and will no longer be innovative.

Phase III

Technology integration plans probably exist at some level in most districts; they will have been developed by teachers, administration, parents, and everyone except the technology staff. It is critical that the technology staff be included when developing the technology integration plan. These plans are an integral part of the district's technology plan, in areas such as budget, yearly goals, and evaluation of previous plans. The target audience for phase III will be technology staff, administration, and K12 faculty.

Major challenges in Phase III will include timeframe and credibility. The technology integration plan is necessary for the technology plan which will be completed again in 2011. Credibility will be an issue because whoever is doing the training will need to have a teaching license. There is not a state requirement, but regardless of I/T experience, without a teaching license teachers are less likely to allow someone to "dictate what gets taught".

Phase IV

An area that the MDE state technology plan lacks is accountability. The state plan defines current status, goals, barriers, and strategies for achieving goals, but does not define metrics for measuring achievement of goals or consequences for not achieving goals. At a state-level, consequences are likely to be tied to funding. At a district-level, there needs to be measurement done in several areas: 1) how well policies are enforced; 2) how well policies met the objectives they were designed for; 3) internal audits to verify that federal and state regulations are being followed; and 4) external audits to verify that federal and state regulations are being followed. There will also need to be training for districts to develop metrics for measurement of other items such as technology integration, effectiveness of technology budget, and quality of service provided by I/T staff.

Training for phase IV will need to be started before the next round of technology plans is completely executed which is estimated to be 2015. The current plans will soon be executed and were not developed as documents which provided minimal if any guidance. The next cycle of plans, 2011-2015, will hopefully provide guidance and goals that need to be evaluated, so staff are able to determine the effectiveness of their plans. Emphasis will be placed on evaluating the technology plan, but it is equally important that security, staffing,

and budget issues are addressed as well. Building metrics based on original goals will be a critical component of phase IV.

REFERENCES

AICPA (2005). Summary of Sarbanes-Oxley Act of 2002. Retrieved July 17, 2005, from http://www.aicpa.org/info/sarbanes_oxley_summary.htm.

Baron, J. & Crooks, S. M. (2005). Academic integrity in web based distance education. *Tech Trends*. 49(2). Retrieved July 17, 2005 from Ebsco.

EDUCAUSE (2005). Effective practices and solutions in security. Retrieved July 17, 2005 from http://www.educause.edu/content.asp?page_id=1246&bhcp=1.

Garthwait, A. & Weller, H. G. (2005). A year in the life: two seventh grade teachers implement one-to-one computing. *Journal of Research on Technology in Education.* 37(4), 361. Retrieved July 17, 2005 from Proquest.

Minnesota Department of Education. (2005). State plan for technology in K12 education. Retrieved January 19, 2008, from http://www.education.state.mn.us/MDE/Accountability_Programs/School_Improvement/School_Technology/Tech_Planning/index.html.

Minnesota Department of Education. (2008a). School districts in the state 2007-2008. Retrieved March 17, 2008 from http://www.education.state.mn.us/mdeprod/groups/InformationTech/documents/Maps/000804.pdf.

Minnesota Department of Education. (2008b). World-class students initiative. Retrieved March 23, 2008, from http://www.education.state.mn.us/mde/About_MDE/News_Center/GovernorsBudgetAgenda/index.html.

Minnesota Department of Employment and Economic Development. (2005a). Labor market profile region 1. Retrieved March 23, 2008, from http://www.deed.state.mn.us/lmi/__shared/assets/region111406.pdf.

Minnesota Department of Employment and Economic Development, (2005b). Labor market profile region 2. Retrieved March 23, 2008, from http://www.deed.state.mn.us/lmi/__shared/assets/region211409.pdf.

O'Neill, J. E. (1995). An interview with Dale LaFrenz. Retrieved March 28, 2008, from http://www.cbi.umn.edu/oh/pdf.phtml?id=177.

University of Minnesota, Controllers Office. (2003). GLBA: Implementation of the safeguards rule. Retrieved July 30, 2005, from http://process.umn.edu/groups/controller/documents/information/glb_safeguards_rule.ppt

U.S. Census Bureau. (2008). Minneosta county selection map. Retrieved March 17, 2008, from http://quickfacts.census.gov/qfd/maps/minnesota_map.html

U.S. Department of Education. (2005a). Family Educational Rights and Privacy Act. Retrieved August 7, 2005, from http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

U.S. Department of Education. (2005b). Executive Summary of the No Child Left Behind Act of 2001. Retrieved July 30, 2005, from http://www.ed.gov/nclb/overview/intro/execsumm.html

U.S. Department of Heath and Human Services. (1996). Health Insurance Portability and Accountability Act of 1996. Retrieved July 30, 2005, from http://aspe.hhs.gov/admnsimp/pl104191.htm

APPENDIX A: ENROLLMENT AND POPULATION DATA

This table displays the enrollment in public K-12 schools in twelve counties in northwestern Minnesota and also displays population for those counties over a similar sixteen-year timeframe.

County	K12 Enrollment in 1991-1992	K12 Enrollment in 2007-2008	Population in 1990	Population in 2006 (est.)	Number of K12 School Districts
Beltrami[1]	7,574	7,404	34,384	43,169	7
Clearwater	1,845	1,487	8,309	8,440	2
Kittson	1,150	748	5,767	4,691	3
Lake of the Woods	761	539	4,076	4,327	1
Mahanomen	1,495	1,403	5,044	5,072	3
Marshall	2,425	1,394	10,993	9,951	4
Norman	1,639	1,174	7,975	6,850	3
Pennington	2,691	2,141	13,306	13,709	2
Polk	6,436	5,131	32,498	31,088	7
Red Lake	994	702	4,525	4,168	3
Roseau	3,418	3,190	15,026	16,201	4

Average change in enrollment: 21.6% decrease
Average change in population: 2.8% decrease

Sources:
http://www.education.state.mn.us/MDE/Data/Data_Downloads/Student/Enrollment/School/

http://quickfacts.census.gov/qfd/states/27000.html

---

[1] Excluded from population and enrollment data. Contains a single city, Bemidji, which has grown despite the rest of the county decreasing in population. Counties surrounding Beltrami county have also experienced growth.

APPENDIX B: SURVEY QUESTIONS AND RESPONSE SUMMARY

N=8

	What best describes your role within your district?	Votes
	Abstain	0
	Administration	0
	Technology Staff	5
	Faculty	2
	Other	1
	- Technology Coordinator about 80% tech and 20 admin	

	How long have you been in your current position?	Votes
	Abstain	0
	Less than 1 year	1
	2 – 4 years	0
	4 – 6 years	2
	6 + years	5

	Do you feel that your district employs policies which clearly provide direction to technology staff? (vs an ad-hoc approach)	Votes
	Abstain	0
	Strongly Agree	0
	Agree	0
	Neutral	5
	Disagree	2
	Strongly Disagree	1

4	For each of the following policies, do you agree the policy exists and is followed in your district. If you are unsure if your district has a policy or know that it does not exist, choose Strongly Disagree.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
	Acceptable Use Agreement	3	5	0	0	0
	Data Retention/ Destruction Policy	0	1	3	1	3
	Disaster Recovery Plan	0	1	5	1	1
	Incident Response Plan	0	2	5	1	1
	Internet Safety Policy	1	6	1	0	0
	Security Policy	0	4	2	2	0
	Password Policy	0	2	3	3	0
	Privacy Policy	0	4	2	1	1
	Technology Plan	3	3	0	2	0

5	Do you have a basic understanding of the following laws and how they could be applied to your district and its technology?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
	Child Internet Protection Act (CIPA)	2	4	2	0	0
	Children's Online Privacy and Protection Act (COPPA)	2	2	4	0	0
	Family Education Rights and Privacy Act (FERPA)	1	2	3	2	0
	Gramm-Leach-Bliley Act (GLBA)	0	0	2	3	3
	Sarbaines-Oxley Act (SOX)	0	0	2	3	3

6	Would you be interested in receiving in training related to I/T policies?	Votes
	Abstain	1
	Strongly Agree	5
	Agree	2
	Nuetral	0
	Disagree	0
	Strongly Disagree	0

APPENDIX C: MSIS PROJECT PLAN

The following are the proposal documents for the MSIS project.

1. Project Plan
2. Work Breakdown Structure and Gantt Chart

MSIS Project Plan

Working Title: Reference Guide for K12 Network and Information Administrators

Introduction

The goal of this project is to create a handbook for network and information administrators in K12 educational institutions, including policy creation, management structure, and frameworks for developing a metric upon which to test policies. Upon completion the handbook will be distributed to K12 institutions in Northwestern Minnesota. This distribution will be done as a marketing tool for the author's personal consulting business.

Problem Statement

Through personal experience working with K12 school districts in Northwestern Minnesota, a need was discovered for a new management approach in several districts. All of them being smaller (less than 1000 students) were still using an ad-hoc approach to managing technology resources including spending, staffing, and training.

Ad hoc management styles are ineffective as they do not properly align themselves with regulations related to K12 schools and I/T. Many K12 school districts are still using an ad hoc approach, are not policy driven, and are uncertain as to the need of policies or a policy-based management style. Corporate America and many higher education institutions have already realized the need for policy-based management for legal compliance, internal accountability, and the ability to set performance standards.

In order to educate K12 district technology staff of the importance of policy-driven management, a handbook will be created which will describe some regulations which directly apply or could be applied to K12 school districts and their technology. This list of regulations is derived from policies written by higher education institutions which reference their possible applicability.

Literature Review

Existing and recent legislation such as the Family Educational Rights and Privacy Act of 1974 (FERPA), No Child Left Behind Act of 2002 (NCLB), and even those not directly related to education such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) Sarbanes-Oxley Act of 2002 (SOX) or Gramm-Leach-Bliley Act of 1999 (GLBA) are initiating changes in the way educational institutions manage information and technology. (US Dept of Ed—FERPA 2005) (US Dept of Ed—NCLB 2005) (US Dept of Heath 1996)

Universities and colleges are often forced to follow the new guidelines imposed by GLBA due to the financial transactions that they are involved with. The University of Minnesota for example has initiated several training programs for its employees. The goal of the programs is not to match up non-public information with each law, but to help employees determine what is and is not non-public information and how to handle it. (University of Minnesota, Controllers Office 2003)

SOX focuses on the correctness of a companies finances with respect to its shareholders, while this again does not directly affect educational institutions, it does provide insight as to the general climate in other business sectors. SOX enforces accountability of management, with large recommendations placed on information technology departments to ensure that only those who need to access data can do so, only those who need to modify data can do so, and ultimately ensure that accounts with proper permissions can only be used by the individuals assigned to them through the use of strong passwords or other authentication mechanisms. (AICPA 2005)

Information technology professionals everywhere are being required to provide assurance to management that systems are secure and that policies are in place to minimize damage done to the organization in the case a security event should occur. With respect to information technology security and education, EDUCAUSE (2005) has published a list of best practices for security in higher education environments. Another front that educational institutions must protect is academic integrity. As online learning proliferates, it becomes increasingly difficult to minimize the risks of academic dishonesty. Baron and Crooks (2005) identify

issues with enforcing academic integrity and online learning as well as several best practices to minimize dishonesty. Garthwait and Weller (2005) discuss how technology is being utilized in K12 classrooms in Maine as well as what barriers teachers face when creating technology enhanced instruction.

Project Layout

There will be two deliverables produced. The first is a report which will extend the research conducted in this project plan beyond a literature review to include a survey which will fully detail the need for the manuscript created. The second is a manuscript for a handbook titled "A Reference Guide for K12 Network and Information Administrators". The following is an outline of the report:

- Introduction
- Background Information
- Problem Statement
- Purpose Statement
- Hypothesis
- Description of Study
- Definition of Terms
- Assumptions
- Literature Review
- Description of Manuscript (how this will fulfill the needs of research conducted)

The components of the handbook are as follows:

- Definition of regulations related to K12 networks and their data
- Frameworks for designing a management structure related to technology
- Frameworks for designing policies which follow the guidelines of regulations
- Frameworks for designing security analysis/audits
- Sample management structures
- Sample policies
- Sample security analysis/audits

Conclusion (Future Work)

There will be three types of information gathering done in order to complete this project. The first is a literature review of related legislation, sample policies, and management theory. The second is a survey of administration and technology staff in K12 districts related to their districts policies. The third is personal interviews with both staff in K12 districts and experts in management, policy creation, and security.

The following is a list of regulations which will be investigated throughout my project:

- Sarbanes-Oxley Act
- Gramm-Leach-Bliley Act
- Heath Insurance Portability and Accountability Act
- Children's Internet Protection Act
- No Child Left Behind Act
- Family Educational Rights and Privacy Act
- and various state regulations such as Minnesota's Government Data Practices Act

The following is a list of common policies which will be investigated throughout my project:

- Acceptable Use
- Security and Password
- Disaster Recovery
- Academic Integrity
- Privacy
- Incident Response (to above policies)

Attached is a proposed timeline for the completion of this project. The goal is to complete and present the project before spring break of the Spring 2008 semester.

References

AICPA (2005). *Summary of Sarbanes-Oxley Act of 2002*. Retrieved July 17, 2005, from http://www.aicpa.org/info/sarbanes_oxley_summary.htm

Baron, J. & Crooks, S. M. (2005). Academic Integrity in Web Based Distance Education. *Tech Trends*. Vol 49. Iss 2. Retrieved July 17, 2005 from Ebsco.

EDUCAUSE (2005). *Effective Practices and Solutions in Security*. Retrieved July 17, 2005 from http://www.educause.edu/content.asp?page_id=1246&bhcp=1

Garthwait, A. & Weller, H. G. (2005). A year in the life: two seventh grade teachers implement one-to-one computing. *Journal of Research on Technology in Education*. Vol 37, Iss 4, p 361 Retrieved July 17, 2005 from Proquest.

University of Minnesota, Controllers Office (2003). *GLBA: Implementation of the Safeguards Rule*. Retrieved July 30, 2005, from http://process.umn.edu/groups/controller/documents/information/glb_safeguards_rule.ppt

University of Minnesota, Controllers Office (2002). *Gramm-Leach-Bliley Act*. Retrieved July 30, 2005, from http://process.umn.edu/groups/controller/documents/index/controller_glba.cfm

University of Minnesota, Policy and Process Development Office (2003). *Rollout of Transaction Justification/Documentation Standards For All Non-Sponsored and Sponsored Transactions*. Retrieved July 30, 2005, from http://www.fpd.finop.umn.edu/groups/ppd/documents/memo/transaction_justification_memo.cfm

U.S. Department of Education (2005). *Family Educational Rights and Privacy Act.* Retrieved August 7, 2005, from http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

U.S. Department of Education (2005). *Executive Summary of the No Child Left Behind Act of 2001.* Retrieved July 30, 2005, from http://www.ed.gov/nclb/overview/intro/execsumm.html

U.S. Department of Heath and Human Services (1996). *Health Insurance Portability and Accountability Act of 1996.* Retrieved July 30, 2005, from http://aspe.hhs.gov/admnsimp/pl104191.htm

ID	Task Name	Duration	Start	Finish
1	**Create Handbook**	21.2 days	Mon 1/28/08	Wed 3/12/08
2	**Regulations and Literature**	4.8 days	Mon 1/28/08	Fri 2/8/08
3	Gather Information	4 hrs	Mon 1/28/08	Fri 2/1/08
4	Compile Information	8 hrs	Fri 2/1/08	Fri 2/8/08
5	**Frameworks for Manual**	4.8 days	Fri 2/1/08	Sat 2/9/08
6	Gather Information	4 hrs	Fri 2/1/08	Sat 2/2/08
7	Compile Information	8 hrs	Sat 2/2/08	Sat 2/9/08
8	Generate Samples	8 hrs	Fri 2/1/08	Wed 2/6/08
9	**Frameworks for Policies**	4.8 days	Wed 2/6/08	Sat 2/16/08
10	Gather Information	4 hrs	Wed 2/6/08	Sat 2/9/08
11	Compile Information	8 hrs	Sat 2/9/08	Sat 2/16/08
12	Generate Samples	8 hrs	Wed 2/6/08	Mon 2/11/08
13	**Frameworks for Security**	4.8 days	Mon 2/11/08	Fri 2/22/08
14	Gather Information	4 hrs	Mon 2/11/08	Fri 2/15/08
15	Compile Information	8 hrs	Fri 2/15/08	Fri 2/22/08
16	Generate Samples	8 hrs	Mon 2/11/08	Sat 2/16/08
17	Prepare Draft	24 hrs	Fri 2/22/08	Wed 3/12/08
18	**Create Report**	7.4 days	Mon 2/25/08	Mon 3/10/08
19	Gather Information	1 wk	Mon 2/25/08	Sat 3/1/08
20	Prepare Draft	10 hrs	Mon 3/3/08	Mon 3/10/08
21	Present to Faculty	4 hrs	Wed 3/12/08	Sat 3/15/08
22	Make Revisions	12 hrs	Sat 3/15/08	Mon 3/24/08

APPENDIX D: HANDBOOK FOR K12 I/T POLICYMAKERS

Guide to Developing K12 Information Technology Policies

Anders Berggren

2008

Contents

1 Issues Facing K12 I/T Departments

This chapter discusses some of the issues facing K12 I/T departments. Three areas of focus will be regulations, staffing, and asset management.

1.1 Regulations

There are a variety of regulations directly impacting K12 school districts and how they use technology. There are obvious connections made between laws such as the Child Internet Protection Act and technology. It is vital to stay current with any regulations directly impacting K12 school districts and their use of technology. Unfortunately there are many other laws which are related to data privacy, accountability of administration, and even the storage of some data which do not directly relate themselves to I/T or K12 school districts. While they may seem irrelevant, they in many cases provide a general atmosphere of the legal issues surrounding I/T and can sometimes be stretched to apply to K12 school districts. In many cases there will be an overlap of the requires each law places on technology systems and those who manage them.

1.1.1 CALEA

The Communications Assistance for Law Enforcement Act was originally written in 1994 by Congress to provide funding to telecommunications providers so they could upgrade their equipment in order to facilitate law enforcement wiretaps. Law enforcement wiretaps were also required to be provided by the Communications Act, but most companies had not invested in equipment with the capacity to provide wiretap or pen register

capabilities.

There have been remarks made in recent years regarding the extension of CALEA in order to allow wiretapping of packet based networks which would include data networks. There were specic exclusion of information networks in the Communications Act, but in updates to CALEA, those have been removed. There have even been attempts to include requirements of back doors into gateway (router) equipment.

While this seems to mainly apply to telecommunications companies, Internet service providers, and possibly hardware vendors there is some application to K12 school district networks. There is a certain level of responsibility assumed by the district when providing Internet access to a wide variety of users. The ability to track with either packet loggers or similar tools the activity of a particular user and determine the history of a particular user is especially important after lawsuits from the RIAA (Recording Industry Artists of America) regarding illegal file sharing. While it is not necessary at this required by law, when designing networks, rewalls, and privacy policies it is benecial to not only internal audits but also to assist law enforcement agencies to do so with the ability to log and review activity in as easy a way as possible.

1.1.2 CIPA

The Child Internet Protection Act is very directly aimed at public schools and libraries. The goal of this law is to protect minor children from inappropriate content found on the Internet. It dictates that in order for schools and libraries to receive various federal grants such as E-Rate and LSTA, that three things must take place.

1. Policy of Internet Safety

   The creation of some district wide policy, whether it be called a policy of Internet safety, acceptable use agreement, or other name of a similar nature which includes operating a technology protection measure in order to protect children and adults from accessing on any Internet-enabled computer connected to the district network against visual depictions considered to be obscene, child pornography, or harmful to minors.

2. Technology Protection Measures

   Installation of some technology specically installed and operated which will block visual depictions considered to be obscene, child pornography, or harmful to minors.

3. Public Notice

   A public hearing at which the Internet safety policy will be discussed before it is implemented.

According to CIPA, harmful to minors means

1. taken as a whole and with respect to minors, appeals to prurient interest in nudity, sex, or excretion;

2. depicts, describes, or represents, in a patently offensive way with what is suitable for minors, an actual or simulated sexual act or sexual contact,

actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. taken as a whole, lacks serious literary, artistic, political, or scientic views as to minors.

While it may seem that this legislation is some way would restrict what school districts can lter, it does not. It sets a minimum requirement, but does state that only such content may be filtered. There also is a statement which allows the creation of a lter bypass mechanism, where the lter can be temporarily disabled for legal reasons including research.

CIPA has been challenged all the way to the Supreme Court for obstructing freedom of speech provided by the rst amendment. The Supreme Court ruled that public libraries can lter content without violating their patrons freedom of speech.

1.1.3 COPPA

Childrens Online Privacy Protection Act of 1998 is directed at online service providers including websites, pen pals, email, message boards, or chat rooms. It requires parental consent of any user who is less than 13 years old. Personal information including the name, email address, phone number, home address, or any other information which could be used to contact physically or online of the child or their parents cannot be collected or used without the consent of the parents. There must also be a privacy policy in place and accessible before registering for the service.

This can impact K12 school districts in several ways. First would be seeking permission from parents of any students under the age of 13 before assigning a district email address or suggesting to the student to register for another online email address or pen pal service. It is not unreasonable for students to reach eighth grade before the age of 13. Secondly this will impact student directories. If a student directory is published, what information can be included without parental consent. Written privacy policies are something many districts do not have in place. It is something worth noting that in the case of COPPA, a separate policy just for online (webpage and email) access may be benecial.

1.1.4 FERPA

The Family Educational Rights and Privacy Act is another law aimed directly toward educational institutions and their students educational data. It allows students (and parents until the student turns 18) the right to inspect their records. This is important so a student or their parents may request any errors be corrected. It also states that under most conditions, a school must have written permission in order to release the information to other organizations. There are exceptions including when students transfer to other schools, court orders, or necessary parties in order to conduct audits. It is important to note that under FERPA directory information (name, address, telephone number, dates of attendance, awards, and place of birth) can be disclosed. Parents or students, who are of age, need to be notied in advance what information will be released, and need to have the option to opt-out of any or all of their information.

Before releasing any student information it is important to remember that FERPA is not the only law that applies, especially if the directory is to be published online. Both parents and students should be aware of what information is to be released through a formal privacy policy. When determining student information systems, it would be benecial to include the ease of providing access to students and parents as part of the criteria used to make a decision.

1.1.5 GLBA

Gramm-Leach-Bliley Act was crafted to protect the privacy of nancial information of customers. While there are three pieces to the act, the two most signicant are the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy rule denes that there needs to be a privacy policy, that customers can opt-out of any legal information sharing between nancial organizations, and that if a company receives nancial data about an individual for a specic purpose that they are only able to use the information for that purpose. The Safeguards Rule create and follow a security policy which define the series of activities used to protect their customers information.

While this may seem irrelevant to K12 school districts, there is a variety of non-public nancial accounts kept on students for activities fees, collections for property damage, and balances for school lunch programs. With regard to school lunch programs there are also free and reduced lunch applications which contain nancial information. Keeping track of where those documents are stored, how long they are stored, how they are disposed of, and who has access to them while they in existence is crucial whether or not they are stored electronically or in a non-electronic format.

GLBA also requires a privacy policy which addresses this information and

how it is shared with other nancial institutions. This privacy policy needs to be readily available to all customers. In the case of most nancial institutions, a copy of the privacy policy will be provided when services are rst offered and generally once a calendar year.

1.1.6 HIPAA

The Health Insurance Portability and Accountability Act was originally crafted in order to make the sharing of medical data more efficient. The original intent was to cut down on misuse of health insurance and allow for medical professionals to share patient information in order to provide better service by encouraging the electronic sharing of information. Congress also dictated certain security requirements on the sharing of information. Patients are able to request access to their le in order to verify and request the correction of any errors. Medical providers are required to have privacy statements, provide them to their clients, and to train their employees. Patients are also given the option to request more condentiality in respect to their information and how it is shared within an organization between staff (doctors and nurses).

Schools often have medical programs where student information is kept. It may be necessary for this information to be stored in a separate le from the students academic records in order to comply with HIPAA. Student information systems in many cases are also used to store and track medical information. It is important that security systems including proper authentication and authorization are in place to ensure only those with proper clearance have access. If medical records are going to be printed, they should be printed to a non-publicly accessible location and be retrieved immediately. Again there is also the privacy policy requirement.

1.1.7 MN Data Practices Act

The Minnesota Government Data Practices Act rst establishes that government data is public information, unless there are federal laws, state statutes, or other classication which determines the data to not be public information. It clearly denes that there need to be methods for the general public to access data which is considered public information. Individuals asked to provide non-public personal data are required to be presented a Tennessen warning which informs the individual how the data will be used and who will have access to it. Organizations are required to protect the integrity of the data.

1.1.8 NCLB

No Child Left Behind means many things to K12 schools right now, a majority of them are negative in the way they are perceived. While there are a variety of requirements imposed on K12 school districts, the basic issue is accountability. How are districts and teachers performing is analyzed primarily using test scores at the moment.

The issue of accountability with respect to the classroom is the focus of NCLB, but it should lead districts to evaluate how e?ective technology is being used to facilitate learning. With students becoming technology dependent, it should not be questioned that technology needs to be used in the classroom. The question becomes how can technology be used to enhance education instead of hindering it? I/T sta? will need to evaluate various products and make decisions as how they can be integrated into existing curriculum. While educators may be uncertain about the future of their profession after this law has been passed, it does require the collection of data which can enable I/T departments to more easily determine if the technology they invest in has the benets they desire.

1.2 Staffing

Staffing I/T departments in K12 schools varies dramatically depending on the goals of the district. When determining how a district can be staffed, budget is generally the limiting factor. The factors that need to be weighed are:

- **Size of district** How many end-users will there be (students, staff, faculty, administration)? Are all of those users in one building, or are they in several buildings? How close are those buildings to each other (few blocks, several miles)?
- **Level of support** How much time will be devoted to each user? This may be different for type of user (students may be expected to get support from their instructors, so they may need less support). Will faculty be given assistance in developing instructional materials? Is technology training for faculty and staff supposed to be developed in-house or will there be external training opportunities? Use the level of support and the size of the district to determine how much support is necessary.
- **Budget** This is generally a fixed factor, but should not be the first factor considered. If you determine what the budget is and then fill in services, the most important or more efficient services may be overlooked. If an ideal level of support is determined first, then it is easier to determine what areas are most important or will provide the

greatest benefit. It is also important to look for grant opportunities or partnerships with other districts. If your district is developing technology training programs, could they be marketed to neighboring districts to offset the expense.

- **Availability** This is an issue to rural districts more than urban districts, but whether or not there is an employee base to draw from or staffing companies will depend on location. In rural areas, it is always great to bring new talent into a community, but with declining enrollment and shrinking communities, it is not always an option.

Districts have used several approaches to solving these issues such as using a full or part-time teacher or administrator as part-time I/T staff, separate full-time I/T staff, and outsourced I/T staff. There is no prescribed solution to staffing I/T departments. It is as unique as the district. Just as long as there is not a set-it-and-forget-it attitude, there needs to be re-evaluations to determine whether or not the current staffing is meeting the needs of the district.

1.3 Asset Management

The first thing that many may think of regarding asset management would be inventory control. Inventory control is just one piece. Inventory lifecycles are also important. Total Costs of Ownership (TCO) is something that the state hopes districts are aware of.

2 Policy Creation

Before policies can be created, it is important to understand what issues are facing K12 I/T. Some of these were discussed in Chapter 1, but there are many more and they are constantly changing and are unique for each district.

While policies are used in almost every organization, there are many misconceptions regarding how to effectively use policies. In many cases policies are considered to be long infallible documents created by legal departments in some legal language which is not understandable by those governed by them. This is the wrong approach to using policies. When used correctly they should ease decision making and automate management tasks.

For the purpose of clarication there is a difference between policies and procedures. Policies are documents which should define what the goals or requirements of an organization are. They should dene a minimum set of goals or requirements set forth by the district for a task or a behavior. On the other hand, procedures dene a sequence of events which should be followed in order to comply with the policies. This means that procedures cannot be written without rst knowing what the policy. Many organizations have unwritten policies that are used in order to create procedures, such as a procedure detailing how software patches are applied to all systems monthly. The problem with having a procedure with no dened policy is there is no clear action if the procedure is not followed. What happens when software patches are not being applied monthly or at all?

While policy-based management styles aide in the effciency of a manager, creating policies is not an easy task. Based on the best practices of others, a policy lifecycle methodology has been created. Note how the last phase of the policy lifecycle returns to the rst phase. Policies should not be static documents, but rather living documents which are continuously visited to

ensure they are properly aligned with district goals.

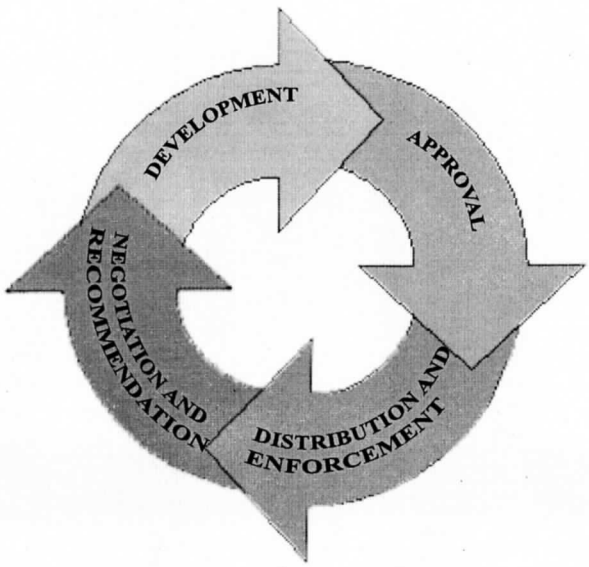


Figure 2.1: Policy Lifecycle

1. **Development**
   The development phase is the most involved and complex, especially if a new policy is being created. The rst step is to determine authors. There needs to be buy-in from various parts of the district, administration, faculty, student/parent, or technology staff depending on who is affected. While those who will be governed by policy may not see the need for formal documentation as to their behaviors, they should be involved. If they are not involved and feel that they have no control over the policies governing them, they are more likely to resist.

   Second, determine what the purpose of the policy is. What is the policy to accomplish? Is there one goal or are there multiple goals?

   Third, determine what the scope of the policy is including the people or systems affected and policies that will either be referenced or modied by the policy. It is critical to fully understand side-effects to the policy. An example would be creating a data destruction policy. As part of a data destruction policy it is likely to be stated, "Any hard drive with private data on it must have multiple passes of random data written over the entirety of the disk before being disposed of or being returned to use in a public location". A side-effect will be asset management planning, what happens when a drive fails with private data on it? Is the drive to be returned for warranty if multiple passes of random data cannot be written to it? If it is not returned

for warranty, what will be done which destroys all data on the disk before it is disposed of?

Fourth, determine who is responsible for enforcing the policy. While in cases such as usage policies, the person enforcing the policy is also governed by the policy, it is not recommended to do this for policies only governing the I/T department in one-man I/T departments. A supervisor should be enforcing the policy. Policies which govern I/T departments should be built into job descriptions. They can be used to determine performance.

Finally, write a draft of the policy. It will need to be reviewed, and there may need to be a legal review.

2. **Approval**
   Administration approval is needed in order for the authority to enact and enforce the new policy. The larger the scope of the policy and the more people it will e?ect, a higher level of administration or school board approval will be needed. eg I/T internal - I/T director, Stu/Fac/Ect - Supt/Prin/BOE

3. **Distribution and Enforcement**
   One the policy has been approved, it needs to be delivered to the people it effects. Part of the delivery process is to educate. Once users are aware of the new policy and reasonable time has been given to adjust their habits, the policy needs to be enforced.

4. **Negotiation and Recommendation**
   After a policy has been in place for some time, it needs to be reviewed to see that it is still e?ective and that it is still aligned with the goals of the district. An example of this would be a password policy may initially state that users may record their secure passwords in a secure location. After users are comfortable with secure passwords the policy may be changed to where users are not allowed to record their passwords anywhere. It is much easier to redevelop a policy than develop a new one from scratch.

When in a policy-making group, there are a few things to keep in mind. A group is necessary for buy-in - must have...

1. Simple Keep policies understandable by all who are required to follow them. Think about who the audience is and what their reading levels are. When writing policies a?ecting elementary students, use a simpler set of wording than writing for faculty.

2. Clear Make sure that what the policy is to accomplish is interpreted correctly. Question if users can determine whether their actions will violate the policy or not. Also dene ambiguous terms such as unacceptable behavior and inappropriate content.

3. Reason It may be clear to those writing policies as to their need, but to other uses it may not be clear why they are necessary. This can be a legal requirement such as an Internet safety policy or a district decision such as a password complexity policy.

4. Scope Know the scope beforehand. Do not cover every possible what if situation, but generalize with statements providing intent and only include pertinent detailed information. Including names of people, software, and costs may require unneeded modications.[?]

3 Example Policies

This chapter includes some sample policies used by the University of Minnesota. The focus of these policies are security. These are the most critical to have in place, in order to address federal and state regulations. Give some background to policy, guideline, standard, procedure. Then an overview of what each of these policies are.

3.1 Account and Password Policy

User Authentication for Access to University Computer Resources

Effective: January 1998
Last Updated: May 2002
Responsible University Officer: Chief Information Officer
Policy Owner: Chief Information Officer

POLICY STATEMENT
The University will provide centrally funded Internet Services to those who are affiliated with the University by using a single source of authentication to provide consistent user identification. Internet Services (including e-mail, internet modem authentication, information storage, etc.) provided by the Office of Information Technology are valuable assets used by students, staff, and faculty engaged in education, research, outreach, and the business of the University. The data accessed using these services and the network are costly resources that must be protected from unauthorized use.

Access to Internet Services provided by the University require use of the

X.500 authentication hub. The X.500 directory will be used as the only source of authentication.

REASON FOR POLICY
The purpose of this policy is:

- To ensure that only authorized individuals are allowed access to central Internet Services on the University network.
- To ensure that we can adequately identify users of Internet Services using University resources.
- To ensure consistent authentication for Internet Services using University network access.
- To conserve and protect University resources.
- To safeguard the integrity of computers, networks, and data of Internet Services.
- To require that departments be responsible for non-student, non-staff individuals to whom they give access.

PROCEDURES
- Applying For Access to the X.500 Directory

FORMS/INSTRUCTIONS
- University of Minnesota Alumni Association Application Form (Call UMAA at 612-624-2323 for a copy of this form.)
- Application for Departmentally Sponsored Email Account

DEFINITIONS
Authenticate
A verification that substantiates that the person is who they say they are. For purposes of this policy, the X.500 directory is used for this verification.

Alumni Qualifications
A member of the University of Minnesota Alumni Association, and
- a graduate of the University of Minnesota
- someone who has attended the University for at least one year in a degree granting program
- a current or past employee of the University of Minnesota.

X.500 Directory
Every student, faculty member, staff person, and affiliate of the University who is entered into the X.500 directory is given a unique X.500 user name. X.500 accounts are created for staff nightly after entry into the PeopleSoft system, and for new students as part of the registration process. Accounts are set up as needed for affiliates of the University. The X.500 Directory is the source for the Student-Staff Directory and on-line look up services.

Sponsored Affiliate Account
A sponsored Affiliated Account is an X.500 account that is purchased for

an affiliate of the University. Normally, sponsored affiliate accounts are established for individuals such as committee workers, volunteers, or contract workers. Departments may purchase sponsored accounts. The department is charged an annual fee for maintaining sponsored accounts.

Internet Services
The Office of Information Technology (OIT) department that provides certain support services in its role as an Internet Service Provider. These services include but are not limited to email, internet modem authentication, and information storage. The services are provided based on the needs of the member of the University community.

University Community
Student, faculty member, staff person, alumni association member, and sponsored affiliate of the University.

RESPONSIBILITIES
System/Network Administrator
Allow only authorized access to Internet Services resources such as computers, networks, and data. Report any security incidents or suspicious activity on local computers, modems, or the network.

Department or College
Be responsible for the activities of individuals sponsored. Ensure that sponsored account users understand and comply with University policies, procedures, and laws relating to conditions of use before authorizing access.

Purchase X.500 accounts for non-student, non-staff individuals who may need access to local computers or the University network. Update account information as needed.

Assurance and Security/Office of Information Technology
Respond to security reports/questions/problems.

RELATED INFORMATION
- Administrative Policy: Acceptable Use of Information Technology Resources
- Administrative Policy: Acquiring a U Card
- Administrative Policy: Internal Access to University Information
- Administrative Policy: Use of University Equipment and Services

HISTORY
Amended: May 2002 - Clarified Policy Statement and Reason, Updated Contacts, Rates, Definitions, Responsibilities, Related Information and Procedure.

Amended: July 2000 - Updated Forms section.

Effective: January 1998

STANDARD–Passwords

Responsible Office: Office of Information Technology
Responsible Officer: Chief Information Officer
EFFECTIVE DATE: November 2006
RELATED POLICY/PROCEDURE:
Acceptable Use of Information Technology Resources

STANDARD
A standard is a level of quality that requires conformity.

Introduction

The Chief Information Officer is designated by the "University Acceptable Use of Information Technology Resources Policy" as the institutional officer responsible to identify standards for access and acceptable use of information technology resources. This standard identifies the minimum password requirements to protect University data and systems. It applies to all electronic devices and systems connected to the University network including computers, network switches and routers, personal digital assistant devices, laptop computers, password authenticated software, etc.

Passwords are used on University devices and systems to facilitate authentication, i.e. helping ensure that the person is who they say they are. The security of University data is highly dependent upon the secrecy and characteristics of the password. Compromised passwords can result in loss of data, denial of service for other users, or attacks directed at other Internet users from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of private data such as private student data, research participant data, and private employee data. To protect against these risks, the Chief Information Officer has approved this standard. Required characteristics of passwords:

- A password or passphrase or other strong authentication must be used for all devices supporting authentication and password authenticated software connected to the University network.
- A password or passphrase must be eight or more characters long. Longer passwords are even better to protect against automated programs that try all the possible combinations of characters (called brute force cracking).
- Passwords or passphrases must be periodically changed as required by each system, but at least annually.
- A password or passphrase must be complex (e.g. include a combination of character types such as numbers, special characters, lower case letters, upper case letters, non-keyboard characters) to help protect against automated cracking.
- A minimum of three types of characters (e.g. lower case letters, numbers, special) should be used for passwords.
- Systems should protect against brute force password guessing programs

from the network and Internet. Whenever possible, systems should lock a user's account if the user fails to login to the system within a specified number of attempts. The lockout may either be for a designated amount of time or until the account is reset.
- Do not share the password assigned to you.
- Adherence to password requirements is reviewed as part of the normal University audit procedures. Collegiate and departmental technology support staff as well as OIT can be contacted for additional questions (contact OIT by dialing 1-HELP, 612-301-4357).

Resources and Links

- Tips for choosing a password: http://www.umn.edu/oit/security/passwordguide.html
- OIT 1-HELP Helpline: http://1help.umn.edu
- Policy links: http://www.umn.edu /oit/policies/index.html

3.2 Incident Response Plan

Reporting and Notifying Individuals of Security Breaches

Effective: May 2006
Last Updated: December 2006
Responsible University Officer: Chief Information Officer
Policy Owner: Chief Information Officer
Policy Contact: Ken Hanna or Tracy Smith

POLICY STATEMENT
The University shall provide timely and appropriate notice to affected individuals when there has been a breach of security of private data about them. A breach in security occurs when there is an unauthorized acquisition of private information maintained in any form by the University. The Chief Information Officer or delegate, in consultation with the General Counsel's Office, shall be responsible for reviewing incidents to determine whether notification is required and directing responsible departments in complying with the notification obligation. All known or suspected breaches of security must be reported to the CIO, to enable the CIO to determine whether notification is required. Suspected breaches can be reported at abuse@umn.edu or your campus help-desk.

REASON FOR POLICY
This policy protects individuals from potential harm arising from the unauthorized acquisition of private information about them, and promotes compliance with state and federal privacy laws.

PROCEDURES

- Reporting Security Incidents and Making Notification (see below)

ADDITIONAL CONTACTS
For questions, contact your unit's IT professional, your campus help-desk, or abuse@umn.edu.

DEFINITIONS
Breach of security
For purposes of this policy this means unauthorized acquisition of data maintained by the University, which compromises the security and classification of the data. Good faith acquisition of government data by an employee, contractor, or agent of the University is not a breach of the security of the data, if the data is not provided to an unauthorized person.

Data
Information collected, stored, transferred or reported for any purpose, whether in computers or in manual files.

Private data
Data about individuals that is classified by law as private or confidential and is maintained by the University in electronic, paper, or other format or medium. Under the Minnesota Government Data Practices Act, " private data" means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data. See Appendix attached to this policy.

Unauthorized acquisition
For the purposes of this policy, this means that a person has obtained University data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-University purposes.

APPENDICES
- Examples of Public, Private, and Confidential Information

FREQUENTLY ASKED QUESTIONS
Q: Where do I report a breach of security?
A: At abuse@umn.edu or your campus help-desk. Look at the attached Procedure for more details on how to report.

Q: What are examples of breaches of security?
A: In the case of electronic data, a breach of security may occur, for example, when a computer containing private data has been hacked and the data has been downloaded, when electronic files have been mistakenly posted on the Web or e-mailed to the wrong recipients, or when a laptop, personal desk assistant, or other electronic storage device has been stolen or lost. In the case of paper data, a breach of security may occur when documents are stolen, lost, misdirected, or left vulnerable to unauthorized acquisition.

Q: Does this policy only apply to electronic data?
A: No, this policy applies to all University data, regardless of the medium.

Q: What if I am aware of a possible incident, but can't tell whether someone has actually acquired the data?
A: You should report the incident, even if you don't know whether someone has acquired the data. The CIO is responsible for determining whether the data has been acquired.

Q: Who makes the notification when there has been a breach?
A: Generally, the department responsible for the data will be responsible for preparing the list of addressees and making the notification, although depending on circumstances the notification may come from someone else at the University. The manner of notification will be determined as part of the consultation process with administrators and the CIO.

Q: Why do we report breaches?
A: For several reasons-to be honest with people about whom we hold data, to help people prevent identify theft when their data is taken, and to comply with legal obligations, including a state law implemented in 2005 requiring notification in certain circumstances.

Q: What should I do if I think my unit is at risk of a breach due to a lack of security?
A: If you think your unit lacks physical or technical security, contact abuse@umn.edu or your campus help-desk.

Q: Will I get in trouble for reporting a breach?
A: No-employees may not be retaliated against for reporting concerns at the University.

RELATED INFORMATION

Statutes
- Minnesota Government Data Practices Act, including Minn. Stat. 13.055
- Minnesota Statutes 325E.61

Policies and Procedures
- Administrative Policy: Protecting the Privacy of Student Education Records
- Administrative Policy: Internal Access to University Information
- Administrative Policy: Acceptable Use of Information Technology Resources
- Administrative Procedure: Reporting Violations of Security, Acceptable Use, Technology Resources, and Threats of Violence (Twin Cities Campuses)
- Administrative Policy: User Authentication for Access to University Computer Resources
- Administrative Policy: Administration and Oversight for Protection of

Individual Health Information
- Administrative Policy: Use and Disclosure of Individual Health Information for Research
- Administrative Policy: Protection of Individual Health Information by University Health Care Components (HIPAA)
- Administrative Policy: Accessing U-Wide Banking Services
- Administrative Policy: Financial Data and Systems Security
- Administrative Procedure: Responding to Security Violations

Other Related Information
- Examples of Public, Private, and Confidential Information - Safe Computing: Identity Theft"

HISTORY
Effective: May 2006

To obtain a copy of a historical policy, e-mail the U Policy Librarian at policy@umn.edu or call 612-624-4372.

Reporting Security Incidents and Making Notification

Related Policies: Reporting and Notifying Individuals of Security Breaches

Last Updated: October 2007
Responsible University Officer: Chief Information Officer
Procedure Contact: See Contacts section of related policy.

PROCEDURE

1. Who should report a breach? Any person who knows or reasonably believes that a breach of the security of private data has occurred should report their concern to the University. Any University employee with responsibility for data must report known or suspected breaches of security of private data. These reports will enable the University to investigate and address the concern and to make determinations about appropriate notification to the subjects of the private data.

2. How do you report a breach? Just send an e-mail to abuse@umn.edu or contact your campus help-desk. Tell them:

- Your contact information
- The department involved
- A brief description of what happened
- A general description of the type of data at issue

3. Who decides whether to notify individuals? The Chief Information Officer (CIO) or delegate, in consultation with the General Counsel's Office, shall be responsible for determining whether a breach of security of data

has occurred and whether notification to individuals is required. The CIO may also seek advice from other key administrators responsible for security and privacy at the University and consult with responsible administrators in the affected campus, area, or unit.

4. How is notification made? The CIO shall work with the affected unit, responsible administrators, University Relations, and others as appropriate to deliver timely and effective notification to individuals. Direct expenses related to the breach notification process are the responsibility of the affected unit. While the content may vary, notification should include:

- A general description of what happened
- The type of private data at issue
- Steps taken to prevent further disclosure of the individual's data
- Contact information for further questions and assistance
- Where appropriate, information to protect against identify theft

3.3 Data Retention and Destruction Policy

STANDARD–Secure Data Deletion

Responsible Office: Office of Information Technology
Responsible Officer: Chief Information Officer
EFFECTIVE DATE: June 2003
RELATED POLICY/PROCEDURE: Acceptable Use of Information Technology Resources

STANDARD
A standard is a level of quality that requires conformity.

INTRODUCTION
The Chief Information Officer is designated by the "University Acceptable Use of Information Technology Resources Policy" as the institutional officer responsible to identify standards for access and acceptable use of information technology resources. This standard defines the use of secure data deletion techniques necessary for the protection of University data and licensed software.

Even though computer users may think that data or programs have been deleted by hitting the "delete key", there are often significant remnants remaining on the hard disk of the computer. Non-public data and licensed software remaining on computers, other electronic devices, and storage media at the time of transfer or disposal represents a substantial risk. To protect against this risk, the Chief Information Officer has approved this standard. Secure Data Deletion

The department or individual directly responsible for non-public data on a University computer or other electronic device is required to ensure that any non-public information on that device is securely removed before sale or transfer out of their direct control. Examples of such sales and transfers are: transfer to another department; public sale; donation; or scrapping. Such computers must be electronically wiped (e.g. using a secure data deletion program for computers that writes random data in multiple passes) or the physical media must be destroyed. Tapes, CDs, cartridges and other storage and backup media containing non-public information must also be securely deleted or destroyed before disposal or transfer out of direct control.

Since it is possible that even systems not thought of as containing important information can have remnants from previous activity, it is recommended that all systems and media moving from one department or type of usage to another be securely wiped. For some types of electronic equipment this may be as simple as pushing the button to return all settings to factory settings. For others, such as computers that are not operational, physical removal and destroying hard disks or other media may be necessary.

The risk mitigation alternative selected should be in proportion to the risk. For most desktop systems with disks that are operational, use of secure data deletion software for three passes would likely be sufficient. With increased risk, increased numbers of passes with the software and the use of physical destruction should be considered. The use of secure deletion tools is reviewed as part of the normal University audit procedures. Collegiate and departmental technology support staff as well as OIT staff can assist in identifying alternatives (contact OIT by dialing 1-HELP, 612-301-4357).

IMPLEMENTATION
The Office of Information Technology (OIT) web site identifies several secure file deletion programs, a few of which are free downloads (see the first listing under Resources below). If a system is non-operational, the disk or other media may still contain non-public data and must be removed and either securely deleted or physically destroyed. Special care should be taken to securely delete or destroy backup and other removable media after use.

In addition to the departmental staff who are responsible for non-public data on their electronic systems, staff involved in any transfers of equipment both within and particularly outside the University through sales, recycling, donations, etc. must be certain that University data and licensed software has been removed. A statement should be obtained from the originating department that non-public data has been removed before making external transfers outside the University.

Upon request, campus technology support groups that perform secure deletion should provide the originating department or user with a form (with identifying information like serial number and the date) and a statement that the campus support group agrees to perform the secure deletion in conformance to the Secure Deletion Standard and assumes responsibility

for doing so.

RESOURCES AND LINKS
- OIT information: Assured Deletion Tools
- OIT helpline: http://1help.umn.edu
- Policy links: http://www.umn.edu /oit/policies/index.html